CMMC 2.0

DARKTRACE

Cybersecurity Maturity Model Certification 2.0

The Cybersecurity Maturity Model Certification 2.0 (CMMC 2.0) is a framework used to assess the cybersecurity posture of contractors and subcontractors working with the US Department of Defense (DoD). It maps specific controls and processes associated with various cybersecurity standards to three maturity models, ranging from basic cyber hygiene to advanced.

The initial version of CMMC (CMMC 1.0) was published by the DoD in September 2020. In November 2021, the DoD announced CMMC 2.0 which included a streamlined model, reliable assessments, and flexible implementation. Specific changes in CMMC 2.0 include the following: reducing the model from 5 to 3 compliance levels; allowing companies at Level 1 and Level 2 to demonstrate compliance through self-assessment; and allowing companies to make Plans of Action & Milestones (POA&Ms) to achieve certification or waive CMMC requirements, both under certain limited circumstances.

CMMC 2.0 has largely been put in place to verify organizational compliance with NIST 800-171 standards and ensures the security of Controlled Unclassified Information (CUI) that resides on DOD industry partners' networks. It will be incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) and used as a requirement for awarding contracts.

The framework is designed to allow smaller businesses to implement the controls associated with lower levels of maturity in a cost-effective and affordable way, while organizations with more resources can build to advanced maturity. Each DOD contract specifies a required level of CMMC 2.0 certification.

It will be critical for all organizations that may affect the security of CUI to have some level of CMMC 2.0 compliance at every level of the contractor supply chain. This requires visibility and cyber defense of CUI across the entire lifecycle of the data and anywhere it may be stored, transmitted, and processed.

Achieving CMMC 2.0 with the Cyber AI Loop

Darktrace delivers AI-powered threat prevention, detection, investigation, and response that can support organizations in their journey towards cyber maturity as defined by the CMMC 2.0 framework. Through a unified platform approach, Darktrace provides autonomous cyber defense across the entire enterprise, including cloud and SaaS, email environments, corporate networks, remote endpoints, and cyber-physical systems.

With Self-Learning AI, Darktrace learns what normal behavior looks like across the business in order to spot the subtle deviations that signal an attack, from novel ransomware to stealthy insiders.

The technology spots emerging threats in real time with Darktrace DETECT, autonomously contains them with Darktrace RESPOND, and takes preemptive action to find vulnerabilities and harden defenses with Darktrace PREVENT – all without relying on any rules, signatures, or prior assumptions. All of these technologies are further supported by the Cyber AI Analyst, which autonomously investigates and triages every potential threat, bringing subtle attacks to light.

Darktrace and CMMC: Framework Applicability

Presented below is a guide showing how Darktrace can assist organizations in working towards CMMC 2.0 practices and associated maturity levels.

For more information on how Darktrace capabilities map to the NIST framework, please see our white paper on Darktrace and NIST.

Domain	Capacity	Number	Description	Darktrace Capability	1	2	3
Access Control	Authorized Access Control	AC.L1-3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Darktrace can enforce access restrictions to tagged systems.	✓		
	External Connections	AC.L1-3.1.20	Verify and control/limit connections to and use of external information systems.	Darktrace can interrupt and prevent data transfer to unauthorized devices.	✓		
	Control Public Information	AC.L1-3.1.22	Control information posted or processed on publicly accessible information systems.	Darktrace discovers internet-facing assets.	✓		
	Control CUI Flow	AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.	Darktrace continuously monitors the flow of information and can enforce restrictions.		✓	
	Separation of Duties	AC.L2-3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Darktrace can detect and interrupt anomalous user activity including SoD violations.		✓	
	Privileged Functions	AC.L2-3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Darktrace can monitor and identify anomalous user activity. This would include anomalous logins from low privileged users.		✓	
	Unsuccessful logon attempts	AC.L2-3.1.8	Limit unsuccessful logon attempts.	Darktrace can autonomously lock cloud accounts after suspected incidents of a brute force attack.		✓	
	Control Remote Access	AC.L2-3.1.12	Monitor and control remote access sessions.	Darktrace allows security teams to see what remote access protocols are being used, and action accordingly.		✓	
	Privileged Remote Access	AC.L2-3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	Darktrace can be used to detect and interrupt anomalous and unauthorized use.		✓	
	Mobile Device Connection	AC.L2-3.1.18	Control connection of mobile devices.	Darktrace automatically identifies device types and continuously monitors and interrupts anomalous device activity.		✓	

Domain	Capacity	Number	Description	Darktrace Capability	1	2	3
Awareness Training	Role-Based Risk Awareness	AT.L2-3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	Darktrace reveals an organizations most at-risk users based on a continuous assessment of attack pathways, and creates AI-generated social engineering attacks to test these attack pathways.		✓	
	Insider Threat Awareness	AT.L2-3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Darktrace creates emulated attack campaigns that reflect the actions of a compromised or malicious insider.		✓	
Audit and Accountability	Event Review	AU.L2-3.3.3	Review and update logged events.	Darktrace reporting functionality includes event metrics which can be used to confirm appropriate coverage.		✓	
	Audit Correlation	AU.L2-3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Darktrace can serve as a centralized point for collection and correlation of logs and network traffic to provide situational awareness of anomalous activity.		✓	
	Reduction & Reporting	AU.L2-3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	Darktrace provides fully automated and on-demand AI investigation of anomalous events.		✓	
	Audit Protection	AU.L2-3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Darktrace uses role-based user access controls to secure information contained within the platform and also continuously monitors and interrupts anomalous data access, modification, and deletion.		✓	

Domain	Capacity	Number	Description	Darktrace Capability	1	2	3
Configuration Management	Security Configuration Enforcement	CM.L2-3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Darktrace can identify security misconfigurations and enforce security settings.		✓	
	Security Impact Analysis	CM.L2-3.4.4	Analyze the security impact of changes prior to implementation.	Darktrace continuously analyzes an organizations risk along with the expected change in risk if certain actions were to be taken.		✓	
	Access Restrictions for Change	CM.L2-3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	Darktrace detects and interrupts anomalous and unauthorized access and use of organizational systems.		✓	
	Nonessential Functionality	CM.L2-3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	Darktrace identifies and interrupts vulnerable and potential nonessential programs, functions, ports, protocols, and services.		✓	
Identification and Authentication	Multifactor Authentication	IA.L2-3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Darktrace can take autonomous action to enforce multi-factor authentication.		✓	
Incident Response	Incident Reporting	IR.L2-3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Darktrace continuously performs AI-based investigation and triage of all anomalies. The results of this analysis are documented and summarized in a report and designated parties are notified.		✓	
Maintenance	System Maintenance Control	MA.L2-3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Darktrace continuously monitors for and autonomously interrupts anomalous activity including activity from maintenance tools.		✓	
Personnel Security	Personnel Actions	PS.L2-3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Users of Darktrace can place certain employees or devices deemed to be high risk on a watch list. Darktrace then increases its sensitivity around these assets. Many organizations use this to provide additional assurance.		✓	

Domain	Capacity	Number	Description	Darktrace Capability	1	2	3
Physical Protection	Monitor Facility	PE.L2-3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	Darktrace supports monitoring and reporting on physical protection systems.		✓	
	Alternative Work Sites	PE.L2-3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	Darktrace coverage can be deployed across all types of work sites.		✓	
Risk Assessment	Risk Assessments	RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	Darktrace continuously assesses and reports on risks associated with an organizations operations, assets, and people.		✓	
	Vulnerability Scan	RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Darktrace continuously monitors assets for known and new vulnerabilities.		✓	
	Vulnerability Remediation	RA.L2-3.11.3	Remediate vulnerabilities in accordance with risk assessments.	Darktrace provides risk-based recommendations for vulnerability remediation and autonomously implements enhanced detection and response for temporary remediation.		✓	
Security Assessment	Security Control Assessment	CA.L2-3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Darktrace continuously monitors organizations internally and externally and can identify the effectiveness of security controls.		✓	
	Security Control Monitoring	CA.L2-3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Darktrace continuously monitors organizations internally and externally and can identify the effectiveness of security controls.		✓	

Domain	Capacity	Number	Description	Darktrace Capability	1	2	3
System and Communications Protection	Boundary Protection	SC.L1-3.13.1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Darktrace continuously monitors organizations internally and externally and can alert on and interrupt unauthorized and/or anomalous activity.	✓		
	Public-Access System Separation	SC.L1-3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Darktrace discovers and reports on all publicly accessible assets of an organization.	✓		
	Network Communication by Exception	SC.L2-3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Darktrace can be configured to interrupt all but explicitly allowed network traffic.		✓	
	Split Tunneling	SC.L2.3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	Darktrace can detect and interrupt split tunneling on remote endpoint.		✓	
	Mobile Code	SC.L2-3.13.13	Control and monitor the use of mobile code.	Darktrace identifies mobile code within organizations and can interrupt anomalous activity involving mobile code.		✓	
	Voice Over Internet Protocol	SC.L2-3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	Darktrace can be used to detect and take action on VoIP technologies.		✓	

Domain	Capacity	Number	Description	Darktrace Capability	1	2	3
System and Information Integrity	Malicious Code Protection	SI.L1.3.14.2	Provide protection from malicious code at appropriate locations within organizational information systems.	Darktrace detects and interrupts anomalous activity and potential malicious software within the network.	✓		
	Security Alerts & Advisories	SI.L2-3.14.3	Monitor system security alerts and advisories and take action in response.	Darktrace provides real-time, AI-driven investigation of anomalous events occuring within the organization and integrated third-party security alerts and notices..		✓	
	Update Malicious Code Protection	SI.L1-3.14.4	Update malicious code protection mechanisms when new releases are available.	Darktrace is constantly updating its understanding of normal to detect subtle anomalies that arise.	✓		
	Monitor communications for Attacks	SI.L2-3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Darktrace provides real-time, AI-driven investigation of all communications traffic occuring within the organization, and integrates with Threat Intelligence technologies.		✓	
	Identify Unauthorized Use	SI.L2-3.14.7	Identify unauthorized use of organizational systems.	Darktrace continuously moni-tors organizational systems and alerts on unusual/unauthorized activities.		✓	

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,100 people around the world and protects over 7,700 organizations globally from advanced cyber-threats.

Scan to
LEARN MORE